IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JAMES GAVER, Defendant.	:	Case No. 3:16-cr-88 JUDGE WALTER H. RICE

DECISION AND ENTRY OVERRULING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE BASED ON UNCONSTITUTIONAL DEPLOYMENT OF GOVERNMENT-SPONSORED MALWARE DUBBED THE "NETWORK INVESTIGATIVE TECHNIQUE" (DOC. #9); OVERRULING DEFENDANT'S MOTION FOR DISCLOSURE OF DISCOVERY (DOC. #14); OVERRULING DEFENDANT'S SECOND MOTION TO SUPPRESS EVIDENCE AND MOTION FOR *FRANKS* HEARING (DOC. #21)

Defendant, James Gaver, a registered sex offender, is charged with numerous counts of possession of child pornography, and knowingly accessing with intent to view child pornography, in violation of 18 U.S.C. § 2252(a)(4)(b) and (b)(2), and knowing receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). This matter is currently before the Court on three pending motions: (1) Defendant's Motion to Suppress Evidence Based on Unconstitutional Deployment of Government-Sponsored Malware Dubbed the "Network Investigative Technique" (Doc. #9); (2) Defendant's Motion for Disclosure of Discovery (Doc. #14); and (3) Defendant's Second Motion to Suppress Evidence

and Motion for *Franks* Hearing (Doc. #21). For the reasons set forth below, all three motions are overruled.

I. Background and Procedural History

In 2014, the Federal Bureau of Investigation ("FBI") began investigating a child pornography website called "PlayPen." This website, which had over 158,000 members and attracted more than 1,500 visitors each day, could be accessed only through the Tor network, a "hidden" network that allows users to mask their identity, IP address, and location. Once members logged onto the PlayPen website with a username and password, they had access to chat rooms, private messaging services and thousands of images of child pornography.

In December of 2014, a foreign law enforcement agency gave the FBI a suspected IP address for the PlayPen website, which the FBI determined was hosted on a server in Lenoir, North Carolina. The FBI obtained a search warrant, seized the server, and placed a copy of it onto a government-controlled server in Newington, Virginia.

On February 20, 2015, prosecutors in the Eastern District of Virginia obtained a search warrant from United States Magistrate Judge Theresa Carroll Buchanan. FBI Special Agent Douglas Macfarlane's warrant affidavit explained that the government wanted to continue operating the PlayPen website from the server in Newington, Virginia, for 30 days in order to locate and identify visitors to the website.

Because the PlayPen website was accessible only through the Tor network, this was not an easy task. In order to obtain the visitors' IP addresses, the government requested authorization to deploy a Network Investigative Technique ("NIT"). Any time a visitor signed onto the PlayPen website, the NIT would force the user's computer, wherever it was located, to collect certain information, including the computer's IP address, and transmit it back to the government-controlled server.[1]

For approximately two weeks, from February 20, 2015, until March 4, 2015, the FBI collected the IP addresses of more than one hundred people who accessed the PlayPen website, including Defendant James Gaver. On February 23, 2015, when he signed onto the PlayPen website, the NIT extracted data from his computer. The government then used this information to obtain his computer's physical address. Five months later, law enforcement officers obtained a traditional search warrant for his apartment in Dayton, Ohio. On July 27, 2015, the government executed the warrant and seized several computers, hard drives, thumb drives, a camera, a cellular phone and other personal property. Mr. Gaver also made several incriminating statements on that date, and again on September 14, 2015.

---

[1] Other information collected included: (1) a unique identifier; (2) the type, version and architecture of the computer's operating system; (3) information about whether the NIT had already been delivered to that computer; (4) the computer's host name; (5) the operating system username; and (6) the computer's Media Access Control address.

On June 16, 2016, James Gaver was indicted on several charges of possession of child pornography, and knowingly accessing with intent to view child pornography, in violation of 18 U.S.C. § 2252(a)(4)(b) and (b)(2), and knowing receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1).

Like dozens of other defendants across the country who were "stung" by the FBI in this operation, Gaver filed a Motion to Suppress Evidence Based on Unconstitutional Deployment of Government-Sponsored Malware Dubbed the "Network Investigative Technique." Doc. #9. He argues that the NIT search warrant issued by the magistrate judge in the Eastern District of Virginia was void, because she had no authority to authorize a search extending beyond the boundaries of the Eastern District of Virginia. Gaver moves to suppress, as "fruit of the poisonous tree," all evidence obtained from the illegal search of his computer, and all incriminating statements he made. But for the issuance of the defective NIT search warrant, the government would not have discovered Gaver's IP address and would not have obtained the warrant to search his apartment.

Pursuant to Federal Rule of Criminal Procedure 16, Gaver also filed a Motion for Disclosure of Discovery. Doc. #14. Gaver asks the Court to order the government to produce "all components to the NIT source code, including the payload, exploit, identifier, and server components."

On October 19, 2016, Gaver filed a Second Motion to Suppress Evidence and Motion for *Franks* Hearing. Doc. #21. In addition to the previously-asserted grounds for suppression, Gaver alleges that key facts in the NIT warrant

application were false, and that the government either omitted or misrepresented other facts that were material to the probable cause determination. He also alleges that the NIT warrant was expressly limited to a location in Virginia, and did not authorize a search of his computer, which was located in Ohio. Finally, he alleges that the NIT warrant is an unconstitutional general warrant.

On January 17, 2017, the Court held a hearing on the pending motions. The parties then filed post-hearing briefs. Docs. ##29, 31. The Court turns first to Defendant's Motion for Disclosure of Discovery.

II. Defendant's Motion for Disclosure of Discovery (Doc. #14)

Gaver asks the Court to order the government to produce "all components to the NIT source code, including the payload, exploit, identifier, and server components." He then wants to hire a computer expert to determine: (1) the full extent of information seized when the NIT was deployed; (2) how the government was able to compromise the computer's security setting; (3) whether the NIT compromised any data or computer functions; and (4) whether the government's representations about how the NIT works are complete and accurate.

Gaver argues that, to the extent any of the charges against him are based on images that were downloaded to his computer *after* February 23, 2015, when the NIT was deployed, he needs the NIT source code to determine whether the NIT could have surreptitiously installed malware that caused those images to be transmitted to his computer, altered those images, or otherwise left his computer

vulnerable to attacks from third parties.[2] At the hearing, defense counsel admitted that this "may sound somewhat farfetched," but argued that "certainly it's not outside the realm of possibility." Hr'g Tr. at 25.

The government is willing to produce: the "payload," which is the instructions sent to Gaver's computer to gather the information; a list of all information collected by the NIT; the two-way network data stream; the computer code used to generate unique identifiers related to the NIT; and a forensic copy of Gaver's computer, which could be examined by an expert. The government maintains that this information is sufficient to allay Gaver's speculative concerns that the NIT may have somehow altered his computer. The government is also willing to let Gaver inspect the report containing a description of his activities on the site during the time the NIT was deployed.

The government, however, is not willing to produce the "exploit" or "server component" of the NIT source code. The "exploit" is the code that was used to circumvent the security features of the Tor browser so that the FBI could run commands on Gaver's computer. The server component stores the information gathered by the NIT. According to the government, the "exploit" and "server component" are immaterial to Gaver's defense and, in any event, are subject to a qualified law enforcement privilege.

---

[2] During a conference call held on February 7, 2017, the government indicated that Counts 4 and 5 involved images that were downloaded after March 4, 2015.

Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government to permit inspection of items within its control if: (1) the item is material to defense preparation; (2) the government intends to use it in its case-in-chief, or (3) the item belongs to the defendant. Only the first condition is at issue here. In order to establish materiality, Gaver must show that pretrial disclosure of this evidence would enable him to significantly alter the quantum of proof in his favor. *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010).

Even if Gaver can show that the information sought is material to his defense, he is not necessarily entitled to it. The government has asserted a qualified law enforcement privilege, applicable when the information sought pertains to sensitive law enforcement techniques and procedures. When such a privilege is asserted, the court must balance the defendant's need for the privileged information against the public interest in nondisclosure. *United States v. Pirosko*, 787 F.3d 358, 365 (6th Cir. 2015); *In re The City of New York*, 607 F.3d 923, 948 (2d Cir. 2010).

Having reviewed the relevant case law, the Court concludes that the exploit and server components of the NIT source code are not material to Gaver's defense and, even if they were, they are subject to the law enforcement privilege. As the government notes, it has offered to produce enough of the NIT source code which, along with the forensic copy of Gaver's computer, would allow a computer expert to determine whether deployment of the NIT rendered Gaver's computer vulnerable to attacks by third parties. Because Gaver has not taken advantage of this offer,

he has no evidence to support his claim that someone else could be responsible for some of the images found on his computer.

When faced with similar circumstances, numerous courts have denied defendant's requests for the entire NIT source code, finding them to be too speculative. *See United States v. Matish*, 193 F. Supp. 3d 585, 599 (E.D. Va. 2016) ("an examination of Defendant's computer may have uncovered evidence either of hacking or an alternate source of the child pornography, but, as it stands, the declarants' inaction leaves their hypotheses with no evidence to support them."); *United States v. Darby*, No. 2:16-cr-036, Doc. # 49, PageID##788-790 (E.D. Va. Aug. 12, 2016) (noting that Defendant failed to take advantage of information offered by the government, and had no evidence to support his hypothetical claim that the FBI had lied about how the NIT worked); *United States v. Jean*, No. 5:15-cr-50087, 2016 WL 6886871, *7 (W.D. Ark. Nov. 22, 2016) (noting that Jean's experts had failed to run any tests on his computer, and holding that he could not "rest his entire argument in support of compelling discovery on a virtually impossible hypothetical situation."); *United States v. Tippens*, No. 3:16-cr-5110, Doc. #106, at 28 (W.D Wash. Nov. 30, 2016) ("Defendants' speculation about what the remaining NIT code could show" was insufficient to compel discovery).

These courts all found that the defendants failed to show that the information sought was material to their defense.[3] As one court noted, "[e]ssentially, the

---

[3] In *United States v. Michaud*, No. 3:15-cr-5351, Doc. # 223 (W.D. Wash. May 25, 2016), the same judge who later decided *Tippens* found that the NIT code was material, but that it was privileged. The court did not force the government to

Defendant requests discovery in order to carry out an impermissible 'fishing expedition,' claiming that he cannot know what evidence he is looking for until he finds it." *United States v. McLamb*, —F. Supp. 3d—, 2016 WL 6963046, *8 (E.D. Va. Nov. 28, 2016). The same is true for Mr. Gaver. He has failed to show how, in light of all of the information that the government has *already* offered him, the exploit and the server component are material to his defense.

Moreover, even if the exploit and server component were material, the government has satisfied its burden of proving that this information is privileged. The Court is persuaded by the government's argument that disclosure of the exploit and server component of the NIT would severely compromise future investigations, and could allow others to develop countermeasures. Courts have widely agreed that these portions of the code are protected by the law enforcement privilege, because the defendant's need for it is greatly outweighed by the government's need to keep it secret. *Darby*, Doc. #49, PageID#789; *Matish*, 193 F. Supp. 3d at 601; *Jean*, 2016 WL 6886871, at *7; *McLamb*, —F. Supp. 3d—, 2016 WL 6963046, *8 n.6.

For these reasons, the Court OVERRULES Defendant's Motion for Disclosure of Discovery, Doc. #14.

---

produce it, but did suppress all evidence obtained as a result of the NIT. To this Court's knowledge, no court other than *Michaud* has found the entire NIT source code to be material to the defense.

III. Defendant's Motion for a *Franks* Hearing (Doc. #21)

Citing a number of alleged defects in the 33-page affidavit that FBI Special Agent Douglas Macfarlane presented to Magistrate Judge Buchanan in support of the NIT search warrant, Gaver has requested a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Doc. #21.

In *Franks*, the Supreme Court held as follows:

> where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Id. at 155–56.

Warrant affidavits are presumed to be valid, and allegations that they contain deliberately false or misleading statements or statements made with reckless disregard for the truth "must be accompanied by an offer of proof." *Id.* at 171. A statement is made "with reckless disregard for the truth" when viewing all the evidence, "the affiant in fact entertained serious doubts as to the truth of the affidavits or had obvious reasons to doubt the accuracy of the information contained therein." *United States v. Cican*, 63 F. App'x 832, 835-36 (6th Cir. 2003).

Gaver argues that several false and misleading statements contained in Agent Macfarlane's affidavit were made knowingly and intentionally, or with reckless disregard for the truth, and that they were material to the finding of probable cause. Gaver maintains that, without these false and misleading statements, the affidavit was insufficient to establish probable cause to believe that any user, wherever located, who signed onto the PlayPen website knew that it was dedicated to child pornography, and knowingly accessed it with intent to view child pornography.

In addition to the exhibits attached to his motion, Gaver was given the opportunity at the January 17, 2017, hearing to proffer arguments and evidence in support of his request for a *Franks* hearing. Agent Macfarlane was present at the hearing to testify on the issue of whether he relied on the warrant in good faith. However, to the extent that some of this testimony overlapped with the question of whether his affidavit contained knowingly false or misleading statements, or statements made with reckless disregard for the truth, the Court will consider it for that purpose also.

Notably, Macfarlane's affidavit has been reviewed by many courts. *See, e.g., Matish*, 193 F. Supp. 3d at 603-07; *United States v. Darby*, 190 F. Supp. 3d 520, 533-34 (E.D. Va. 2016); *United States v. Allain*, —F. Supp. 3d.—, 2016 WL 5660452, at *7-8 (D. Mass. Sept. 29, 2016); *United States v. Owens*, No. 16-cr-38, 2016 WL 7079609, at **5-7 (E.D. Wis. Dec. 5, 2016). None has found sufficient cause to hold a *Franks* hearing. For the reasons set forth below, this Court

likewise finds that Gaver has failed to show that the alleged inaccuracies meet the standard for a *Franks* hearing.

A. False Description of PlayPen's Homepage

Paragraph 12 of Macfarlane's February 20, 2015, affidavit describes the homepage of the Play Pen website as follows: "On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." Gov't Ex. 1. At the hearing, Macfarlane testified that this was the logo that appeared every time he viewed the homepage from September of 2014 through February 18, 2015. He did not access the site again between February 18, 2015, and February 20, 2015, when he submitted the warrant application. Hr'g Tr. at 72-76.

It is undisputed that, sometime in that two-day period, the logo was changed. On February 20, 2015, the homepage showed just one girl, perhaps slightly older than the girls previously depicted, wearing a short dress, fishnet stockings and posed in a sexually suggestive manner. Ex. C. Although one of the other agents may have signed onto the website on February 19, 2015, and observed this change, no one told Macfarlane about it. Hr'g Tr. at 75.

Gaver argues that the false statement in Macfarlane's affidavit was material to a finding of probable cause because, with the new logo, it was far less evident that this was a website dedicated to child pornography. He notes that the PlayPen name is also associated with adult pornography websites and periodicals. Ex. H.

He also claims that the new logo was similar to many mainstream pictures of child models. Ex. I.

Gaver has not shown that the false statement was made knowingly and intentionally or with reckless disregard for the truth. Given that the logo had remained unchanged for months, Gaver's failure to access the website one last time prior to submitting the affidavit may have been somewhat negligent, but it cannot be deemed reckless.

Moreover, in the Court's view, the old logo and the new logo are not materially different. As the other courts have found, both logos are highly suggestive of the website's illegal contents, particularly when paired with the website's name, and the fact that it was accessible only through the Tor network. *See Matish*, 193 F. Supp. 3d at 606-07; *Darby*, 190 F. Supp. 3d at 534; *Allain*, —F. Supp. 3d.—, 2016 WL 5660452, at *8; *Owens*, 2016 WL 7079609, at *6. In short, even with an accurate description of the website's logo, probable cause would have existed for the issuance of the warrant.

B. Other False or Misleading Statements Related to PlayPen's Homepage

Gaver maintains that other statements contained in Macfarlane's affidavit, although "technically true," were presented in such a way as to create a false impression that anyone who found the PlayPen website was inevitably looking for child pornography.

For example, Macfarlane states that the website's "primary purpose is the advertisement and distribution of child pornography." Gov't. Ex. 1, at ¶11. Gaver

notes, however, that the website is also a chat forum. Arguably, someone could access the site for the sole purpose of exercising their right to engage in protected speech.

Macfarlane describes the homepage as stating "No cross-board reposts, .7z preferred, encrypt filenames, include preview." Gaver maintains that these statements are not necessarily indicative of criminal activity, although Macfarlane presents them as such. For example, Macfarlane states that, based on his training and experience, he knows that "no cross-board reposts" refers to a prohibition against reposting material from other websites, and .7z "refers to a preferred method of compressing large files or sets of files for distribution." *Id.* at ¶12.

Gaver also challenges Macfarlane's suggestion that one cannot access the PlayPen website without knowing the exact URL address, and his statement that "[a]ccessing the [PlayPen website] therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble across the [PlayPen website] without understanding its purpose and content." *Id.* at ¶10. Gaver maintains that, because the Tor network has its own search engine and indices, someone could, in fact, stumble across the PlayPen website by searching for legal content such as "sex chat" or "teen erotica."

Gaver has failed to make a preliminary showing that Macfarlane intentionally sought to mislead the magistrate judge either by making these statements, or by leaving out critical information that would have defeated a finding of probable cause. *See United States v. Khami*, 362 F. App'x 501, 505-06 (6th Cir. 2010).

As the court noted in *McLamb*, although it is possible that someone could innocently stumble across the PlayPen website, "[i]t is improbable that anyone would go to the trouble of registering for the site in order to look for [legal content] likely available elsewhere on the Internet." —F. Supp. 3d—, 2016 WL 6963046, at *5. As the government points out, probable cause is supported by the fact that PlayPen is accessible only through the Tor network, its suggestive name, the sexually suggestive photos of the young girls on the homepage, and the warnings to users to remain anonymous when registering.

C. Misleading Statements About the Website's Content

Given that the NIT was deployed as soon as a user logged on to the PlayPen website, Gaver argues that Macfarlane's statements about what was available *after* a user logged on are largely irrelevant to the probable cause determination. Gaver also argues that those statements are misleading, because many "commonplace" features of the website, such as the ability to upload photographs and videos that are accessible only to registered users of the website, or the ability to exchange names and messages with other users on a Tor-based instant messaging service, Gov't Ex. 1, ¶¶15, 23, 24, are not necessarily indicative of criminal activity. Gaver argues that these statements were included in order to mask the absence of probable cause to search the computers of all individuals who accessed the PlayPen website.

The Court disagrees. For the reasons set forth above, the Court finds that, even if these allegedly misleading statements are set aside, the remaining content

of Macfarlane's affidavit is sufficient to show that probable cause exists to believe that the search would uncover evidence of criminal activity.

D. False and Misleading Statements About the Location of the NIT Searches

Gaver also argues that the warrant affidavit contains false and misleading statements about the location of the NIT searches. He notes that the cover sheet indicates that the property to be searched is located in the Eastern District of Virginia. It also refers to Attachment "A," which states that the server operating the website in question is "located at a government facility in the Eastern District of Virginia." Gov't Ex. 1.

Gaver claims that these statements are false and misleading. Although the NIT was deployed from the server that was located in the Eastern District of Virginia, the actual property to be searched, *i.e.*, the target computers, was scattered across the United States and abroad. Gaver maintains that Macfarlane's affidavit does not make this clear. It makes it appear that the server itself is the object of the search. According to Gaver, Macfarlane made these statements in an attempt to deceive the magistrate judge, who would have known that she had no authority to issue a warrant that extended beyond the boundaries of her own district.

The Court disagrees. Macfarlane's affidavit must be read as a whole. Although the "fill in the blank" cover sheet states that the property at issue is located in the Eastern District of Virginia, the cover sheet also refers to

Attachment "A," which states that, after the NIT is deployed, it will obtain information from the activating computers. "The activating computers are those of *any user or administrator who logs into* the TARGET WEBSITE by entering a username and password." Gov't Ex. 1 (emphasis added). In addition, Macfarlane's affidavit describes how the NIT will cause the activating computer, "wherever located," to transmit certain information to a government computer to help identify the location of the activating computer and its user. *Id.* at ¶¶33-37, 46. These statements clearly indicate that data will be gathered from computers located outside of the Eastern District of Virginia.

Gaver has failed to make a substantial preliminary showing that any false or misleading statements knowingly and intentionally, or with reckless disregard for the truth, were included in Macfarlane's warrant affidavit. He has also failed to make a substantial preliminary showing that the allegedly offending statements were necessary to the magistrate judge's finding of probable cause. Accordingly, the Court OVERRULES Gaver's Motion for a *Franks* Hearing, Doc. #21.

IV. Defendant's Motions to Suppress Evidence (Docs. ##9, 21)

Gaver argues that, for various reasons, the NIT warrant resulted in an illegal search and seizure of identifying information from his home computer. He has filed a Motion to Suppress, as "fruit of the poisonous tree," all evidence obtained by the FBI when it executed the derivative residential search warrant on July 27, 2015, and other incriminating statements he made to law enforcement officers on

September 14, 2015. Doc. #9. Gaver's motion was supplemented by a Second Motion to Suppress Evidence, Doc. #21.

The Sixth Circuit has held that individuals may have a reasonable expectation of privacy in the contents of their home computers. *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). The government concedes that the deployment of the NIT to extract information from Gaver's computer constituted a "search" within the meaning of the Fourth Amendment. *See* Doc. #27, PageID#543 n.2.

A. Federal Rule of Criminal Procedure 41(b)

1. Magistrate Judge Had No Authority to Issue NIT Warrant

Gaver contends that the February 23, 2015, search of his computer was unconstitutional, because Magistrate Judge Buchanan had no authority under the Federal Magistrates Act, 28 U.S.C. § 636, or under Federal Rule of Criminal Procedure 41(b), to issue the NIT warrant, authorizing a search outside the boundaries of the Eastern District of Virginia. The Court agrees.

Within the district where a magistrate judge is appointed, he or she has "all powers and duties" conferred by the Federal Rules of Criminal Procedure. 28 U.S.C. §636(a)(1). In turn, Federal Rule of Criminal Procedure 41(b), as it existed on the date the NIT warrant was issued, gave magistrate judges authority to issue a warrant:

(1) "to search for and seize a person or property located within the district;"

(2) "for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;"

(3) "for a person or property located within or outside that district," if connected to a terrorism investigation where related activities may have occurred in the district;

(4) "to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both;" and

(5) on some federal property, regardless of where it is located, if the criminal activity occurred within the district of the issuing magistrate judge.

Fed. R. Crim. P. 41(b).

Gaver maintains that the NIT warrant fell outside the scope of these provisions. This Court now joins the majority of other courts that have held that the magistrate judge lacked authority to issue the NIT warrant under Rule 41(b). *See, e.g., United States v. Werdene*, 188 F. Supp. 3d 431, 441 (E.D. Pa. 2016) ("Even a flexible application of the Rule . . . is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections."); *United States v. Ammons*, —F. Supp. 3d—, 2016 WL 4926438, at *5 (W.D. Ky. Sept. 14, 2016) ("Magistrate Judge Buchanan had no authority to issue the NIT warrant."); *United States v.*

Levin, 186 F. Supp. 3d 26, 34 (D. Mass. 2016) (concluding that Rule 41(b) did not authorize issuance of the NIT warrant); *United States v. Michaud,* No. 3:15-cr-5351, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (holding that Rule 41(b) "does not directly address the kind of situation that the NIT Warrant was authorized to investigate"); *United States v. Arterbury*, No. 15-cr-182, 2016 U.S. Dist. LEXIS 67091, at *22 (N.D. Okla. April 25, 2016) ("the NIT warrant was not authorized by any of the applicable provisions of Rule 41"); *United States v. Adams*, No. 6:16-cr-11, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) (holding same); *Allain*, —F. Supp. 3d—, 2016 WL 5660452, at *11 ("the NIT warrant did not comply with Rule 41(b)"); *United States v. Croghan*, Nos. 1:15-cr-48, 1:15-cr-51, 2016 U.S. Dist. LEXIS 127479, at *18 (S.D. Iowa, Sept. 19, 2016) ("Magistrate Judge Buchanan lacked authority to issue the NIT Warrant pursuant to any provision of Rule 41(b)."); *United States v. Scarbrough*, No. 3:16-cr-35, 2016 U.S. Dist. LEXIS 141373, at *26 (E.D. Tenn. Aug. 26, 2016) (holding that the magistrate judge lacked authority to issue a warrant to search property located outside of her district); *United States v. Workman*, No. 15-cr-397, 2016 U.S. Dist. LEXIS 133782, at *13 (D. Col. Sept. 6, 2016) (same).

A handful of courts have found that issuance of the NIT warrant was authorized under Rule 41(b)(4), which permits a magistrate judge to issue a warrant to "install within the district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both." These courts have reasoned that the NIT was akin to a "tracking device" that was

installed in the Eastern District of Virginia to track the movement of information when the users logged onto PlayPen. *See, e.g., United States v. Jones*, No. 3:16-cr-26, Doc. #60 (S.D. Ohio February 2, 2017) (Rose, J.) (finding that the NIT operated as a virtual tracking device, and that the search took place in Virginia); *United States v. Jean*, —F. Supp. 3d —, 2016 WL 4771096, at *17 (W.D. Ark Sept. 13, 2016) (holding that the NIT was "not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception."); *Darby*, 190 F. Supp. 3d at 536 ("Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site."); *Matish*, 193 F. Supp. 3d at 612 (referring to a "virtual trip" to Virginia via the Internet); *McLamb*, —F. Supp. 3d—, 2016 WL 6963046, at *6 (finding the NIT analogous to a tracking device); *United States v. Austin*, —F. Supp. 3d—, 2017 WL 496374, at *4 (M.D. Tenn. Feb. 2, 2017) (same); *United States v. Sullivan*, No. —F. Supp. 3d—, 2017 WL 201332, at *5 (N.D. Ohio Jan. 18, 2017) (same).

The Court finds these cases unpersuasive. The NIT software did not "track" the movement of a "person or property" as those terms are commonly construed. Instead, it searched for information. *See Adams*, 2016 WL 4212079, at *6 ("the NIT does not track; it searches."); *Croghan*, 2016 U.S. Dist. LEXIS 127479, at *15 (finding that the NIT "did not 'track' the 'movement' of anything."). Nor does the NIT "install" anything on the activating computer "in the sense that nothing was left behind after the NIT finished"); it simply gathers information and relays it back to the government-controlled computer. *See United States v. Kahler*, No. 16-

cr-20551, 2017 WL 586707, at *6 (E.D. Mich. Feb. 14, 2017). Because this information goes far beyond providing location information, "[t]he NIT is more than just a 'tracking device'; it is a surveillance device." *Id.* *See also Allain*, —F. Supp. 3d—, 2016 WL 5660452, at *11 ("Given that the 'activating' computers never entered the Eastern District of Virginia, it stretches the rule too far to say that the installation occurred within the Eastern District of Virginia."). Based on the plain language of this Rule, subsection (b)(4) is inapplicable.

Notably, on December 1, 2016, Rule 41(b) was amended to expand the authority of a magistrate judge to issue something akin to the NIT warrant:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Fed. R. Crim. P. 41(b)(6). On February 20, 2015, however, Magistrate Judge Buchanan lacked authority to issue such a warrant. This rendered the warrant void *ab initio*.

2. Suppression is Not an Appropriate Remedy for the Rule 41(b) Violation

Given that the NIT warrant was void, the search of Gaver's computer was akin to a warrantless search. Because none of the recognized exceptions to the warrant requirement applies (*i.e.*, consent, exigent circumstances, etc.), the search was *per se* unreasonable and violated the Fourth Amendment. *See United States*

v. Hudson, 405 F.3d 425, 441 (6th Cir. 2005). Gaver argues that, because the search violated his constitutional rights, all fruits of the illegal search must be suppressed.[4] *See Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963). This is not necessarily so. As the Sixth Circuit noted in *United States v. Master*, "the decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred." 614 F.3d 236, 242 (6th Cir. 2010) (citing *Herring v. United States*, 555 U.S. 135, 141 (2009)).[5]

In *Herring*, the Supreme Court acknowledged that the exclusionary rule, "when applicable, forbids the use of improperly obtained evidence at trial." *Id.* at 139. This judicially-created rule exists to deter violations of the Fourth Amendment. *Id.* at 140. Nevertheless, even when a Fourth Amendment violation is found, "suppression is not an automatic consequence." *Id.* at 137.

The exclusionary rule applies only when the benefits of deterrence outweigh the costs to society. *Id.* at 141. "To trigger the exclusionary rule, police conduct

---

[4] In the alternative, Gaver argues that if the Court finds that issuance of the NIT warrant *technically* violated Rule 41(b), but did not rise to the level of a constitutional violation, he has nevertheless established the requisite prejudice to justify suppression of the evidence. He contends that, but for the wrongful issuance of the NIT warrant, his computers would not have been seized and he would not have been charged with these crimes. Because the Court finds that Gaver's Fourth Amendment rights were, in fact, violated, it does not reach this alternative argument.

[5] "The question whether the exclusionary rule's remedy is appropriate in a particular context has long been regarded as an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct." *Illinois v. Gates*, 462 U.S. 213, 223 (1983).

must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. Accordingly, under the good faith exception to the exclusionary rule, evidence that is obtained under a search warrant that is later invalidated will not be suppressed if the officers acted in objectively reasonable reliance on that warrant. *United States v. Leon*, 468 U.S. 897, 922 (1984).

Gaver contends that the government's deliberate disregard of the jurisdictional restrictions placed on magistrate judges by Rule 41(b) justifies suppression. He further argues that, because the warrant was void *ab initio*, the good faith exception to the exclusionary rule cannot be applied. The Court rejects both of these arguments.

Gaver notes that, as early as 2013, a magistrate judge in Texas had rejected a similar warrant application because it was outside the scope of Rule 41(b). *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Texas 2013). Thereafter, largely because of that holding, the Department of Justice ("DOJ") began seeking changes to the Rule. These efforts ultimately led to the December 1, 2016, amendment expressly authorizing the issuance of warrants to use remote access to search electronic storage media and seize electronically-stored information located within or outside the district. *See* Fed. R. Crim. P. 41(b)(6). Gaver argues that, based on this history, there is no doubt that the DOJ knew that the NIT warrant it was requesting from Magistrate Judge Buchanan was unlawful.

At the hearing, however, Special Agent Macfarlane credibly testified that, prior to submitting the warrant affidavit, he was not aware that courts had denied similar warrant requests. Nor was he aware that the DOJ was lobbying to expand the scope of a magistrate judge's authority under Rule 41(b) to encompass such a request. Hr'g Tr. at 77-78. When he presented Magistrate Judge Buchanan with the warrant affidavit, he believed that she had authority to sign it; after she did, he "absolutely" believed he had a valid warrant. *Id.* at 54.

In the Court's view, despite the fact that the magistrate judge lacked authority to issue the NIT warrant, suppression of the evidence obtained as a result of that warrant is not justified in this case. The odds that suppression would deter future violations by law enforcement officers are very low. There is no evidence to support a finding that Macfarlane deliberately or recklessly invited Magistrate Judge Buchanan to exceed the bounds of her authority. Notably, numerous courts across the country have held that Rule 41(b) *did* authorize Magistrate Judge Buchanan to issue the NIT warrant. If the courts themselves cannot agree on this issue, it can hardly be said that law enforcement officers acted in bad faith in seeking the warrant. *See Austin*, —F. Supp. 3d—, 2017 WL 496374, at *8 ("there is nothing in the record in this case indicating that the FBI agents who sought the NIT Warrant deliberately, recklessly, or with gross negligence, selected a magistrate judge who did not have territorial jurisdiction under Rule 41 to issue the warrant.").

Moreover, as many courts within the Sixth Circuit have noted, Macfarlane did what he was required to do. He gathered evidence, and then submitted a very detailed warrant affidavit, explaining exactly how the NIT would work, including the fact that it would gather information from the computer of anyone who logged onto the PlayPen website, regardless of where they were located. *See Sullivan*, 2017 WL 201332, at *8 (finding that the FBI agents acted in good faith); *Ammons*, —F. Supp. 3d—, 2016 WL 4926438, at *9 (same); *Kahler*, 2017 WL 586707, at *8 ("this is not a case where the FBA purposely avoided compliance with the law."); *Scarbrough*, 2016 U.S. Dist. LEXIS 141373, at **33-34 (concluding that the deterrent value to law enforcement is low).

In addition, to the extent that the NIT warrant was improperly issued, the blame lies not with the law enforcement officers, but with the magistrate judge. As the Supreme Court has noted, "[t]he exclusionary rule was crafted to curb police rather than judicial misconduct." *Herring*, 555 U.S. at 142. Moreover, because Rule 41(b) has been amended to explicitly allow the issuance of such warrants, there is no longer any need to "deter" even the magistrate judges. *See Sullivan*, 2017 WL 201332, at *8; *Austin*, —F. Supp. 3d—, 2017 WL 496374, at *8 ("To the extent there was an error in determining the parameters of Rule 41's territorial jurisdiction, that error rests with the magistrate judge, not with the agents. Under these circumstances, there is little deterrent value to be gained through suppression.").

While the deterrent value of suppression is low, the cost to society is very high. As shown in all of these cases, individuals involved in the dark underworld of child pornography go to great lengths to avoid detection. But for tools like the NIT, law enforcement officers may never be able to identify these individuals to bring them to justice. *See Ammons*, —F. Supp. 3d—, 2016 WL 4926438, at *9 (noting that society has a significant interest in deterring child pornography); *Scarbrough*, 2016 U.S. Dist. LEXIS 141373, at *36 ("individuals accessing the Playpen website were victimizing the most vulnerable members of society, children, and were using the anonymizing technology of the Tor to evade detection.").

The Court finds that the costs to society of suppressing the evidence are significantly outweighed by the benefit of deterrence. Moreover, the Court finds that the good faith exception to the exclusionary rule applies in this case.

In *Levin*, the District Court of Massachusetts held that the good faith exception was not available in cases where the warrant was void *ab initio* because the judge lacked authority to issue it. 186 F. Supp. 3d at 40. The court went on to say that, even if the good faith exception could be applied, suppression would be justified because it was not objectively reasonable for Macfarlane to believe that the magistrate judge had authority to issue the NIT warrant. *Id.* at 42. *See also Arterbury*, 2016 U.S. Dist. LEXIS 67091, at *34 ("where the Rule 41 violation goes directly to the magistrate judge's fundamental authority to issue the warrant, . . . the warrant is void *ab initio*, suppression is warranted and the good-faith

exception is inapplicable."); *Croghan*, 2016 U.S. Dist. LEXIS 127479, at **26-27 (holding that suppression was appropriate, and that the good faith exception did not apply); *Workman*, 2016 U.S. Dist. LEXIS 133782, at *24 ("where the issuing judge acts outside her authority the good-faith exception should not apply.").[6]

These cases, however, are contrary to Sixth Circuit authority. Gaver relies on *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001), in which the court held that where the retired judge who signed the warrant lacked authority to do so, the good faith exception could not apply.

In *United States v. Master*, however, the Sixth Circuit held that *Scott* was no longer viable in light of the recent Supreme Court authority that "effectively created a balancing test." 614 F.3d 236, 242-43 (6th Cir. 2010) (citing *Herring*, 555 U.S. 135, and *Hudson v. Michigan*, 547 U.S. 586 (2006)). Although it was undisputed that the judge in *Master* lacked authority to issue the search warrant at issue, the Sixth Circuit held that this did not necessarily foreclose application of the good faith exception. *Id.* In order to suppress evidence, the benefits of deterrence must outweigh the cost to society. The court noted that, "[a]rguably, the issuing magistrate's lack of authority has no impact on police misconduct, if

---

[6] Gaver also relies on a Report and Recommendation recently issued in *United States v. Carlson*, Crim. No. 16-317 (D. Minn. March 23, 2017), in which the magistrate judge recommended that the court find that the good faith exception cannot apply when the warrant is void *ab initio*. *See* Second Supp. Auth. to Defendant's Sealed Motion to Suppress at Docket #9. Doc. #32. A Report and Recommendation has no precedential value unless and until adopted by the district court but, in any event, like the other cases cited by Gaver, this Report and Recommendation is contrary to Sixth Circuit authority.

the officers mistakenly, but inadvertently, presented the warrant to an incorrect magistrate." *Id.* at 242.[7]

To this Court's knowledge, every court within the Sixth Circuit that has been asked to suppress evidence obtained as a result of the NIT warrant has found that the good faith exception to the exclusionary rule applies, following the *Herring* and *Master* line of decisions. *See Sullivan*, 2017 WL 201332, at *8; *Austin*, —F. Supp. 3d—, 2017 WL 496374, at *8; *Ammons*, —F. Supp. 3d—, 2016 WL 4926438, at *9; *Kahler*, 2017 WL 586707, at *8; *Scarbrough*, 2016 U.S. Dist. LEXIS 141373, at *33-36; *Jones*, No. 3:16-cr-26, Doc. #60, PageID#808 (S.D. Ohio Feb. 2, 2017) (Rose, J.); *United States v. Stamper*, No. 1:15-cr-109, Doc. #48, PageID#294 (S.D. Ohio, Feb. 19, 2016) (Barrett, J.). Likewise, numerous courts outside of the Sixth Circuit have held that the good faith exception applies. *See Allain*, —F. Supp. 3d—, 2016 WL 5660452, at *11; *Darby*, 190 F. Supp. 3d at 538; *Michaud*, 2016 WL 337263, at *7; *United States v. Anzalone*, —F. Supp. 3d—, 2016 WL 5339723, at *10 (D. Mass. Sept. 22, 2016); *Werdene*, 188 F. Supp. 3d at 451-52.

The Court finds that the officers acted in objective good faith reliance on the NIT warrant. As previously discussed, given that courts have widely split on the

---

[7] In *Master*, the Sixth Circuit remanded the case so that the district court could re-examine the facts and balance the competing interests as required in *Herring*. On remand, the district court held that suppression was not warranted. The Sixth Circuit agreed, finding that the officer's actions were "neither deliberate nor sufficiently culpable that suppression would be warranted to deter similar behavior in the future." *United States v. Master*, 491 F. App'x 593, 597 (6th Cir. 2012).

question of whether Rule 41(b) authorized Magistrate Judge Buchanan to issue the NIT warrant, it cannot be said that Macfarlane's belief that the warrant was valid was objectively unreasonable. Accordingly, suppression is not warranted.

In Gaver's Second Motion to Suppress Evidence, Doc. #21, he asserts two additional grounds for suppression: (1) the search of his computer in Ohio was not authorized by the NIT warrant; and (2) the NIT warrant was an unconstitutional, general warrant. The Court turns now to a brief discussion of those two grounds.

B. Search of Gaver's Computer Was Authorized by NIT Warrant

Gaver contends that, because the cover page of the search warrant application lists only the Eastern District of Virginia as the location of the property to be searched, the search of his computer, which was located in the Southern District of Ohio, fell outside the scope of the NIT warrant.

The Court rejects this argument for reasons previously discussed. Although the Eastern District of Virginia is listed as the location of the property to be searched, the cover page also refers to Attachment A, which is entitled "Place to be Searched." Gov't Ex. 1. Attachment A makes it clear that, although the computer server was located in Virginia, the NIT would operate to obtain information from the activating computers of "any user or administrator who logs into the TARGET WEBSITE." *Id.* Implicit in this statement is the concept that these "activating computers" may be located outside of the district. *See Michaud*, 2016 WL 337263, at *4 ("A reasonable reading of the NIT Warrant's scope gave

the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto [the PlayPen website]."); *Owens*, 2016 WL 7079609, at **8-9 (same); *United States v. Jean*, No. 5:15-cr-50087, 2016 WL 4771096, at **11-12 (W.D. Ark. Sept. 13, 2016) (finding that the NIT warrant met the particularity requirement of the Fourth Amendment). Moreover, the body of Macfarlane's affidavit describes how the NIT will cause each activating computer, "wherever located," to transmit certain information to a government computer. Gov't Ex. 1 at ¶46.

C. NIT Warrant Was Not an Unconstitutional General Warrant

Finally, Gaver argues that the evidence must be suppressed because the NIT warrant was an unconstitutional, general warrant that allowed the FBI "to conduct a massive number of computer searches on unidentified targets in unknown locations." Doc. #21, PageID#482. He contends that the warrant is not sufficiently specific. Numerous courts have rejected this argument. *See, e.g., Michaud*, 2016 WL 337263, at *5; *Darby*, 190 F. Supp. 3d at 533; *Matish*, 193 F. Supp. 3d at 607-08; *United States v. Acevedo-Lemus*, No. SACR15-137, 2016 WL 4208436, at *7 n.4; *Jean*, 2016 WL 4771096, at *11–12; *Anzalone*, —F. Supp. 3d—, 2016 WL 5339723, at *7; *Allain*, —F. Supp. 3d—, 2016 WL 5660452, at *8–9; *Owens*, 2016 WL 7079609, at *7. This Court finds that the NIT warrant sufficiently describes particular places and things to be searched, *i.e.*, the computers of anyone who logged onto the PlayPen website.

Gaver further argues that this broad warrant was not supported by probable cause. However, for the reasons explained above, the Court finds that there was ample probable cause to believe that evidence of criminal activity would be found on the computer of each individual who logged onto the PlayPen website. This was not an unconstitutional general warrant.

V. Conclusion

For the reasons set forth above, the Court OVERRULES Defendant's Motion for Disclosure of Discovery, Doc. #14. The Court also OVERRULES Defendant's Motion to Suppress Evidence Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," Doc. #9, and Defendant's Second Motion to Suppress Evidence and Motion for *Franks* Hearing, Doc. #21.

Date: March 27, 2017

WALTER H. RICE
UNITED STATES DISTRICT JUDGE